PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 696.05-PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US01/13848	International filing date *(day/month/year)* 26 APRIL 2001	Priority date *(day/month/year)* 08 NOVEMBER 2000
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/00, 9/32 and US Cl.: 713/150, 200, 201		
Applicant SRI INTERNATIONAL		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 AUGUST 2001	01 OCTOBER 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LY V. HUA Telephone No. (703) 305-9684

Form PCT/IPEA/409 (cover sheet) (July 1998)★

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US01/13848

I. Basis of the report

1. With regard to the elements of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-8 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the claims:
pages 9-11 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the drawings:
pages 1-2 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/~~fig~~ NONE

5. [ ] This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US01/13848

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	1-18	YES
	Claims	NONE	NO
Inventive Step (IS)	Claims	1-18	YES
	Claims	NONE	NO
Industrial Applicability (IA)	Claims	1-18	YES
	Claims	NONE	NO

2. citations and explanations (Rule 70.7)

Claims 1-18 meet the criteria set out in PCT Article 33(2)-(4), because:

1. with regard to claims 1-12, the prior art does not teach or suggest a secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender and the recipient sharing a secret encryption key and an expected nonce value comprising:
   a. generating a new nonce value known to the sender;
   b. encrypting the message including the expected nonce value and the new nonce value, using the encryption key;
   c. transmitting the encrypted message from the sender to the recipient; and
   d. verifying, by the recipient, that the encrypted message includes the expected nonce value;

2. with regard to claims 1-12, the prior art does not teach or suggest a system for managing communications within a network collaboration group, comprising:
   a. means for generating a new nonce value;
   b. means for incorporating an expected nonce value and the new nonce value in a message to be transmitted;
   c. means for encrypting the message;
   d. means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and
   e. means for verifying, by the recipient node, that the encrypted message includes the expected nonce value;

3. with regard to claims 1-12, the prior art does not teach or suggest a data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master and the member, the signal comprising:
   a. the information to be transmitted;
   b. an expected nonce value known to the master and the member; and

(Continued on Supplemental Sheet.)

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):

c. a new nonce value, different than the expected nonce, provided by a sender of the signal; and

4. with regard to claims 1-12, the prior art does not teach or suggest a method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:

a. encrypting messages using a key shared by the master and the member, so as to protect confidentiality of the message; and

b. embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages.

---------- NEW CITATIONS ----------

NONE